Appendix I

Frequently Asked Questions about Quantum Cryptography

« SECOQC Business White paper »
http://www.secoqc.net/downloads/SECOQC_Business_Whitepaper_01b.pdf

1. **Do I need quantum cryptography?**

That depends on the importance given to informational assets. Two important components have to be considered:

- The security level the currently mechanism offer,
- The value of the information to be protected and security criteria to be fulfilled.

In some critical infrastructures like governmental and administrative applications, financial domains, energy sector installations etc. the need of a robust technology offering a high security level is something mandatory.

Taking into account that computer power drastically increases in a continuous way and that there is no mathematical proof of its cryptographic algorithms' robustness, asymmetrical cryptography could be considered as potentially insecure in the near future.

2. **Do international regulations require the use of quantum cryptography?**

No regulation requires explicitly the use of quantum cryptography but regulations (such as SoX and Basel II) regarding the financial domain require exactitude and reliability for the financial statement. However what is required is to protect informational assets in the best way, which could be differently interpreted according to the context. Quantum cryptography is a solution satisfying legal compliance and certifying that information is correctly protected.

3. **Is QKD expensive?**

It depends on what "expensive" does mean in a particular context. Currently, adopting a QKD technology has a good Return On Investment for many reasons:

- QKD will remain secure for a long time because of its physical properties;
- there is no need for frequent upgrades which is a very expensive aspect in a long run vision;
- there is no disruption of business during upgrade, which is more expensive than QKD itself.

The implementation of a new and innovative technology could generate cost due principally to hardware costs.

But it is not to be neglected that cost can be reduced in the long term by massive market adoption.

4. **Why do I need to change my present cryptographic system?**

First of all you do not need to change your present cryptographic system. QKD is for generating and distributing secure keys for your existing cryptographic applications, but also for your future applications. In that way the adoption of a QKD will improve significantly the quality and the security level of communication.

5. **How to integrate quantum cryptography in my existing IT infrastructure?**

The high speed QKD system can be integrated into a fibre optical telecom infrastructure, such as a Local Area Networks (LAN) or Metropolitan Area Networks (MAN) to enable secure communication and information exchange among users.

It could be installed in parallel to the running system, and then eventually been plugged in.

Another way is to wrap the QKD system around your existing systems.

6. **Does QKD need dedicated optical fibre?**

QKD's network implementation needs dedicated fibre currently. With up to 1000 strands in contemporary fibres, dedicated fibres are not a very costly problem. In spite of this, the future development could allow the use of wavelength-division multiplexing (WDM). It is a technology, which multiplexes multiple optical carrier signals on a single optical fibre by using different wavelengths (colours) of laser light to carry different signals. This allows a multiplication in capacity, in addition to enabling bidirectional communications over one strand of fibre.

Alternatively, free space QKD can be applied where photons are exchanged between two telescopes (see below).

7. **Is it possible to use QKD on a copper fibre?**

QKD explicitly cannot be use on copper fibre, but the use of a quantum number generator to design a key session (as described in the e-voting application of the Geneva Canton - CH) is possible over a copper fibre.

8. **Is QKD possible in free space?**

The possibility to operate QKD in free space was demonstrated on multiple occasions (1998: 1 km in the US, 2001: 1.9 km in the UK, 2002: 10 km in the USA). In 2003 photons were exchanged in the Alps in Germany at a distance of 23 km. In 2005 it was reported that Chinese scientists succeeded in an inner-city free-space distribution of entangled photon pairs over a distance of 10.5 km. About the same time, an experiment was published where entangled photons were distributed directly through the atmosphere to a receiver station in 7.8 km distance in the City of Vienna. In 2007 a quantum key was established between ESA telescopes on two of the Canary Islands over a distance of 144 km. The quality of the free space transmission is highly depending on atmospheric conditions.

9. **Is it possible to use QKD within a Local Area Network (LAN)?**

A local area network implementation of QKD is already operational to connect one or more remote sites by a QKD link. The transmission distance can be increased beyond 100 km by chaining links.

10. **What is the distance limitation?**

For a point-to-point connection the distance limitation is about 100 km in order to obtain reliable quality of the signal. The SECOQC's network architecture allows to overpass this physical constraint and to extend the capacity of QKD transmission over a wide area network (WAN).

11. Which are the principal domains in which a QKD network might be useful?

Quantum key generation and distribution answer high security needs and can for example be used to secure transmissions in the following areas:

- Government or military entities
- Banks and financial institutions (Interbank-Transfer, communications Bank to ATM, …);
- Critical infrastructures,
- Telecoms operators;
- Airports;
- Etc.

12. Can end users benefit from quantum cryptography?

Any end user disposing of an optical fibre infrastructure can benefit from the Quantum Cryptography advantages to enhance the security level of their transmission.